Practitioner's Docket No. NAI1P091/01.049.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Jeffrey Green et al.

Application No.: 09/935,635 Group No.: 2143
Filed: 08/24/2001 Examiner: Neurauter, G.
For: SYSTEMS AND METHODS FOR MAKING ELECTRONIC FILES THAT HAVE BEEN CONVERTED TO A SAFE FORMAT AVAILABLE FOR VIEWING BY AN INTENDED RECIPIENT

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on July 3, 2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed November 13, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P091).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P091).

/KEVINZILKA/
Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
	)	
Green et al.	)	Group Art Unit: 2143
	)	
Application No. 09/935,635	)	Examiner: Neurauter, George C.
	)	
Filed: August 24, 2001	)	Date: December 13, 2006
	)	
For: SYSTEMS AND METHODS FOR MAKING ELECTRONIC FILES THAT HAVE BEEN CONVERTED TO A SAFE FORMAT AVAILABLE FOR VIEWING BY AN INTENDED RECIPIENT	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on July 3, 2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review mailed November 13, 2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, a pending appeal noted February 03, 2006 in application serial number 09/935,634 may be, but is not necessarily, related.[

Since no decision(s) has been rendered in such proceeding(s), no material is included in the Related Proceedings Appendix appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-9, 11-34, and 36-43

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-9, 11-34, and 36-43
3. Claims allowed: None
4. Claims rejected: 1-9, 11-34, and 36-43
5. Claims cancelled: 10, 35

C. CLAIMS ON APPEAL

The claims on appeal are: 1-9, 11-34, and 36-43

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1-2, a method carried out by a computer when executing computer-readable program code is provided. In use, an electronic file intended for delivery from a sender (e.g. see item 110a of Figure 1, etc.) to an intended recipient (e.g. see item 110d of Figure 1, etc.) is received. The electronic file has a first file format with a first file extension. Further, it is determined whether the electronic file represents at least a potential security risk to a computer system. If it is determined that the electronic file represents at least the potential security risk, a notification is forwarded to the intended recipient indicating that the electronic file represents at least the potential security risk.

Additionally, a request to view the contents of the electronic file is received from the intended recipient (e.g. see item 110d of Figure 1, etc.). The electronic file is converted (e.g. see item 204 of Figure 2, etc.) from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension. The second file format with the second file extension prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient (e.g. see item 110d of Figure 1, etc.). The electronic file is converted in response to a determination that the electronic file represents at least the potential security risk to the computer system. Furthermore, the converted electronic file is made available for viewing (e.g. see item 206 of Figure 2, etc.) by the intended recipient. See, for example, page 5, paragraph [0013]; pages 7-8, paragraphs [0017]–[0018]; and page 9, paragraph [0021]; and page 13, paragraph [0026] et al.

With respect to a summary of Claim 4, as shown in Figures 1-2, a method carried out by a computer when executing computer-readable program code is provided. In use, an electronic file intended for delivery from a sender (e.g. see item 110a of Figure 1, etc.) to an intended recipient (e.g. see item 110d of Figure 1, etc.) is received. The electronic file has a first file format with a first file extension. The electronic file is converted (e.g. see item 204 of Figure 2, etc.) from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension. The second file format with the second file extension ensures that a computer virus in the electronic file is unable to

harm a computer of the intended recipient (e.g. see item 110d of Figure 1, etc.). The electronic file is converted in response to a determination that the electronic file represents at least a potential security risk to the computer (e.g. see item 204 of Figure 2, etc.). Additionally, a uniform resource locator is forwarded to the intended recipient of the electronic file. The uniform resource locator identifies at least an address of a web page containing the converted electronic file. See, for example, page 5, paragraph [0013]; pages 7-8, paragraphs [0017]–[0018]; page 9-11, paragraphs [0021]-[0024]; and page 13, paragraph [0026] et al.

With respect to a summary of Claim 6, as shown in Figures 1-2, a method carried out by a computer when executing computer-readable program code is provided. In use, a certain electronic file intended for delivery from a sender (e.g. see item 110a of Figure 1, etc.) to an intended recipient (e.g. see item 110d of Figure 1, etc.) is received. The electronic file has a first file format with a first file extension. The certain electronic file is converted (e.g. see item 204 of Figure 2, etc.) from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension. The second file format with the second file extension prevents a computer virus in the certain electronic file from executing when the converted electronic file is opened by the intended recipient (e.g. see item 110d of Figure 1, etc.). The electronic file is converted in response to a determination that the electronic file represents at least a potential risk to the computer. Additionally, the converted electronic file is made available for viewing (e.g. see item 206 of Figure 2, etc.) by the intended recipient. See, for example, page 5, paragraph [0013]; pages 7-8, paragraphs [0017]–[0018]; page 9-11, paragraphs [0021]-[0024]; and page 13, paragraph [0026] et al.

With respect to a summary of Claim 31, as shown in Figures 1-2, a method is provided. In use, a request is received to view the contents of an electronic file infected with a computer virus. The electronic file has a first file format with a first file extension. The electronic file is converted (e.g. see item 204 of Figure 2, etc.), in response to the request, from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension. The second file format with the second file extension prevents the computer virus from executing when the converted electronic file is opened (e.g. see item 208 of Figure 2, etc.). The electronic file is converted (e.g. see item

204 of Figure 2, etc.) in further response to a determination that the electronic file represents at least a potential security risk to a computer. See, for example, page 5, paragraph [0013]; pages 7-8, paragraphs [0017] – [0018]; page 9-11, paragraphs [0021]-[0024]; and page 13, paragraph [0026] et al.

With respect to a summary of Claim 33, as shown in Figures 1-2, a computer-readable medium having instructions stored thereon is presented. When executed by a computer, the instructions cause the computer to convert (e.g. see item 204 of Figure 2, etc.) an electronic file from a first format with a first file extension to a second file format with a second file extension, where the electronic file is intended for delivery from a sender (e.g. see item 110a of Figure 1, etc.) to an intended recipient (e.g. see item 110d of Figure 1, etc.). The second file format with the second file extension is different from the first file format with the first file extension and prevents a computer virus in the electronic file from executing when the converted electronic file is opened (e.g. see item 208 of Figure 2, etc.) by an intended recipient of the electronic file (e.g. see item 110d of Figure 1, etc.). The electronic file is converted (e.g. see item 204 of Figure 2, etc.) in response to a determination that the electronic file represents at least a potential risk to the computer. Additionally, the instructions cause the computer to make the converted electronic file available for viewing (e.g. see item 206 of Figure 2, etc.) by the intended recipient (e.g. see item 110d of Figure 1, etc.). See, for example, page 5, paragraph [0013]; pages 7-8, paragraphs [0017] – [0018]; page 9-11, paragraphs [0021]-[0024]; and page 13, paragraph [0026] et al.

With respect to a summary of Claim 40, as shown in Figures 1-2, an apparatus is presented. The apparatus includes a computer having means for receiving a certain electronic file intended for delivery from a sender (e.g. see item 110a of Figure 1, etc.) to a intended recipient (e.g. see item 110d of Figure 1, etc.). The certain electronic file has a first file format with a first file extension and contains a computer virus. The computer further includes means for converting (e.g. see item 204 of Figure 2, etc.) the certain electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension. The second file format with the second file extension prevents the computer virus from executing when the converted electronic file is opened (e.g. see item 208 of Figure 2, etc.) by the intended recipient (e.g. see item 110d of Figure 1, etc.). The electronic file is converted (e.g. see item 204 of Figure 2, etc.) in response to a determination that

a electronic file represents at least a potential security risk to the computer. The computer further includes means for making the converted electronic file available for viewing (e.g. see item 206 of Figure 2, etc.) by the intended recipient. See, for example, page 5, paragraph [0013]; pages 7-8, paragraphs [0017]–[0018]; page 9-11, paragraphs [0021]-[0024]; and page 13, paragraph [0026] et al.

Of course, the above citations are merely possible examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 29, and 37 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Issue # 2: The Examiner has rejected Claims 1-3, 6, 8-9, 11-21, 23-34, 36-37, and 39-43 under 35 U.S.C. 102(b) as being anticipated by Ji et al. (U.S. Patent No. 5,889,943).

Issue # 3: The Examiner has rejected Claims 4, 5, and 7 under 35 U.S.C. 103(a) as being unpatentable under Ji et al. (U.S. Patent No. 5,889,943) in view of Rudd et al. (U.S. Patent Publication No. 2002/0120693).

Issue # 4: The Examiner has rejected Claims 22, and 38 under 35 U.S.C. 103(a) as being unpatentable under Ji et al. (U.S. Patent No. 5,889,943) in view of Chen et al. (U.S. Patent No. 5,832,208).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 29, and 37 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Group #1: Claims 29, and 37

With respect to claims 29, and 37, the Examiner has specifically argued that appellant's claimed "determining if the first file format is…a graphics file format type…the second file format being…the HTML file format type without scripts…if it is determined that the first file format is the graphics file format type" is not described in the specification to enable one to make and/or use the invention. Appellant respectfully points out paragraph [0025] in the specification, by way of example. Such excerpt discloses and enables converting a file with a graphics file format to an HTML file format and that an HTML file format (without scripts) is a safe format type.

In the Office Action mailed 04/18/2006, the Examiner has argued that "the specification does not enable the conversion of a graphical file format to a HTML file format." Appellant respectfully disagrees and asserts that the claimed technique to "determine if the first file format is one of a word processing format type and a graphics format type… the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type" (emphasis added), as claimed by appellant, is supported and enabled in the specification. For example, paragraph [0025] of the specification states "that the second file having the graphics file format will be converted to a JPB file format, a BMP file format, a JPEG file format, a GIF file format, or a HTML file format" (emphasis added). Additionally, paragraph [0025] of the specification states that "[i]n a further embodiment, the code is configured such that the server computer 122b converts every received electronic file, regardless

of format, to one safe format, such as a HTML file format," which includes files of a graphics format type.

Regarding the Examiner's argument that "the HTML file format is a programming language that defines the structure of a document, not a graphical file," appellant respectfully asserts that HTML file formats are clearly capable of including graphics information. Thus, there is nothing non-enabling with respect to appellant's claimed invention.

Issue # 2:

The Examiner has rejected Claims 1-3, 6, 8-9, 11-21, 23-34, 36-37, and 39-43 under 35 U.S.C. 102(b) as being anticipated by Ji et al. (U.S. Patent No. 5,889,943).

Group #1: Claims 1, 3, 6, 8-9, 11-20, 27-28, 30-34, 36, and 40-43

With respect to each of the independent claims, the Examiner has relied on Col. 11, line 14-Col. 12, line 67, and specifically Col. 12, lines 47-49 and 56-67 in Ji to make a prior art showing of appellant's claimed "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient, said converting of the electronic file being in response to a determination that the electronic file represents at least the potential security risk to the computer system" (see the same or similar, but not necessarily identical language in the above independent claims).

Appellant respectfully asserts that such excerpts only teach "transfer[ring] the mail message with the encoded portions…[with] the viruses deleted…[and] renam[ing] the encode portions of the message containing viruses, [and] stor[ing] the renamed portions as files…and notify[ing] the user of the renamed files and directory path" (emphasis added). Thus, Ji teaches deleting the virus infected portions of a mail message or putting the virus infected portions in a new file and renaming the file. Clearly, since only portions of the file are renamed in Ji, such does not meet appellant's claimed "converting the electronic file." Furthermore, Ji only teaches that such

infected portions are renamed and stored in files. Simply renaming a file does not meet any sort of converting the format of a file in the manner specifically claimed by appellant, and especially not where the conversion "prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient" (emphasis added), as claimed.

In the Office Action mailed 04/18/2006, the Examiner has argued that 'the conversion of the electronic file from a first file format to a second file format includes removing the virus from the attachment which may be in a graphical or word processing format and storing a "treated version" of the file in a format described in Ji as wherein the attachment is "completely cleaned" which includes "removing the virus from the message" and wherein "the infected attachment…may be replaced with the treated version".' However, merely cleaning the attachment and removing a virus from the message or replacing the infected attachment with the treated version simply fails to even suggest "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension" (emphasis added), as claimed by appellant.

In the Office Action mailed 04/18/2006, the Examiner has further argued that 'the "conversion" that is performed as defined [in] the claim may be done on portions of the file as disclosed in Ji as admitted by the Applicant.' It appears that the Examiner is, in his arguments, relying on appellant's specification to interpret the claimed term "conversion." First, it is noted that appellant claims "converting," not "conversion." Further, in response to the Examiner's proposed claim construction, appellant respectfully asserts that such term should be interpreted under its plain and ordinary meaning, as evidenced by the exemplary definition below, insofar as it is not inconsistent with the specification.

> **convert**
> n.
>
> To change (something) into another form, substance, state, or product; transform: convert water into ice.
> To change (something) from one use, function, or purpose to another; adapt to a new or different purpose: convert a forest into farmland.
>
> *The American Heritage® Dictionary of the English Language, Fourth Edition*

However, even if the Examiner erroneously relies on the foregoing interpretation of the term "convert," appellant respectfully asserts that the Examiner has still not taken into consideration the full weight and context of such claimed "converting," as noted above. For example, the Examiner has admitted that "Ji discloses that the file retains its original format, the only difference being that the virus is removed." Thus, by virtue of the Examiner's own admission that Ji's file retains its original format, Ji can not even suggest "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension" (emphasis added), as claimed by appellant.

In the Office Action mailed 04/18/2006, the Examiner has also argued that "[a]s shown within Ji, the virus is removed, thereby preventing the computer virus from executing when the converted electronic file is opened by the intended recipient." However, appellant respectfully points out that appellant claims "converting the electronic file… to a second file format with a second file extension that is different from the first file format with the first file extension and that prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient" (emphasis added), as claimed by appellant. On the other hand, as mentioned above, Ji merely teaches deleting the virus infected portions of a mail message or putting the virus infected portions in a new file and renaming the file. Deleting and renaming virus infected portions does not even suggest "converting the electronic file… to a second file format with a second file extension… that prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient" (emphasis added), as claimed by appellant.

In the Office Action mailed 04/18/2006, the Examiner has additionally argued that "the claims do not specifically require how the electronic file formats are different from each other." The Examiner continued by 'interpret[ing] this difference wherein the first file format with a first file extension is infected with a virus and the second file format is the same file with the virus removed and is considered to be a "safe format" different from the infected format in accordance with the disclosures of the specification.' Again, appellant respectfully disagrees and asserts that

the Examiner's argument improperly dismisses appellant's claimed "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension" (emphasis added), as claimed by appellant. Ji fails to disclose (especially in view of the Examiner's own admission above) that the second file extension is different from the first file extension, in the context claimed by appellant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Ji reference, as noted above.

Group #2: Claim 2

With respect to Claim 2, the Examiner has relied on Col. 17, lines 29-36 in Ji to make a prior art showing of appellant's claimed "said converting occurring in response to said receiving the request to view the contents of the electronic file."

Appellant respectfully asserts that the excerpt from Ji relied upon by the Examiner merely discloses that "[o]nce the retrieval module 283 has stored the message including attachment items in the data buffer 284, the retrieval module 283 signals the virus analysis and treatment module 286 that the information in the data buffer can be analyzed for viruses" (Col. 17, lines 29-33 – emphasis added). In addition, appellant notes that Ji discloses that "[t]he retrieval module 283 preferably includes routines for acquiring data from messages that are found to be unscanned by the polling module 282" and when "an unscanned message is found, the retrieval module 283 preferably downloads the message from the postal node 282 into the data buffer 284 portion of memory 248 of the client node 230" (Col. 17, lines 18-23 – emphasis added). However, the mere disclosure of a retrieval module that acquires and stores data from messages

found to be unscanned by the polling module and then signals the virus analysis and treatment module that the data can be analyzed for viruses, as in Ji, simply fails to even suggest that "said converting occurring in **response** to said receiving the request to view the contents of the electronic file" (emphasis added), as claimed by appellant. Clearly, signaling a virus analysis and treatment module after finding an unscanned message simply fails to even suggest that "converting occurring in response to said receiving the request to view" (emphasis added), in the manner as claimed by appellant.

Again, the foregoing anticipation criterion has simply not been met by the Ji reference, as noted above.

Group #3: Claim 21

With respect to Claim 21, the Examiner has relied on Col. 11, line 14-Col. 12, line 67; Col. 13, lines 15-23; and specifically Col. 11, lines 48-52 and Col. 12, lines 47-49 and 56-67 in Ji to make a prior art showing of appellant's claimed "receiving a second electronic file intended for delivery from another sender to another intended recipient, the second electronic file having a third file format and containing another computer virus; converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient; and making the converted second electronic file available for viewing by the another intended recipient."

Appellant respectfully asserts that such excerpt does not even suggest a file format, as claimed by appellant, but instead only relates to transmitting a message from the client to the server and the use of a postal node to store messages for forwarding or retrieval. Appellant also respectfully asserts that such claims are not met by the prior art for the reasons argued above with respect to Issue #2, Group #1.

Again, the foregoing anticipation criterion has simply not been met by the Ji reference, as noted above.

Group #4: Claims 23-26, and 39

With respect to Claims 23, and 39, the Examiner has relied on Col. 13, lines 21-23; Col. 14, lines 30-38; and Col. 20, lines 22-29 in Ji to make a prior art showing of appellant's claimed "second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format."

Appellant respectfully asserts that such excerpts only relate to the original format of the message, and not to a second file format in the context claimed by appellant, namely where the electronic file is converted from a first file format to the second file format, in the specific manner claimed.

Appellant notes that in the Office Action mailed 04/18/2006, the Examiner failed to address appellant's arguments and merely reiterated the previous rejection. Thus, appellant emphasizes that Ji does not meet appellant's specific claim language.

Again, the foregoing anticipation criterion has simply not been met by the Ji reference, as noted above.

Group #5: Claims 29, and 37

With respect to Claim 29 et al., the Examiner has relied on Col. 13, lines 21-23; Col. 14, lines 30-38; and Col. 20, lines 22-29 in Ji to make a prior art showing of appellant's claimed "determining if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, the HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type" (see the same or similar, but not necessarily identical language in the foregoing claims).

Appellant respectfully asserts that such excerpts only relate to an original format of the file, and do not even suggest any sort of converting a file from one format to another, let alone in the specific manner claimed by appellant.

Appellant notes that in the Office Action mailed 04/18/2006, the Examiner again failed to address appellant's arguments and merely reiterated the previous rejection. Thus, appellant emphasizes that Ji does not meet appellant's specific claim language.

Again, the foregoing anticipation criterion has simply not been met by the Ji reference, as noted above.

Issue # 3:

The Examiner has rejected Claims 4, 5, and 7 under 35 U.S.C. 103(a) as being unpatentable under Ji et al. (U.S. Patent No. 5,889,943) in view of Rudd et al. (U.S. Patent Publication No. 2002/0120693).

Group #1: Claims 4,and 5

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that it would have been obvious to combine Ji with Rudd because "the references are directed to converting electronic files between formats in order to disable computer viruses" and because "one of

ordinary skill would have been motivated to combine these references and would have considered them to be analogous to one another based on their related fields of endeavor." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Ji and Rudd references, especially in view of the vast evidence to the contrary.

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.).

Appellant respectfully notes that the Ji reference "relates to a system and method for detecting and removing computer viruses" (Col. 1, lines 12-14 – emphasis added). On the other hand, the Rudd reference primarily teaches "a conversion service for converting attachments to e-mails sent to a client of the service into a format readable by the client" (paragraph [0007]) in order to overcome "compatibility problems [that] may exist between different platforms or software packages" (paragraph [0003] – emphasis added). Accordingly, appellant respectfully disagrees with the Examiner's argument that it would have been obvious to combine the Ji and Rudd references because such references are directed to converting electronic files between formats in order to disable computer viruses," especially in view of the different problems the Ji and Rudd references address, as noted above (emphasis added). Similarly, appellant respectfully asserts that the process of removing computer viruses, as in Ji, is not analogous to addressing compatibility problems, as in Rudd, contrary to the Examiner's arguments. Thus, appellant respectfully asserts that there would have been no suggestion or motivation to combine the aforementioned references.

Additionally, appellant respectfully asserts that the Rudd reference teaches "converting attachments to e-mails sent to a client of the service into a format readable by the client" (paragraph [0007] – emphasis added). On the other hand, the Ji reference teaches "transfer[ing] the mail message unchanged," "transfer[ing] the mail message with… portions… deleted from the mail message," "renam[ing] the encode portions of the message containing viruses, stor[ing] the renamed portions as files…notify[ing] the user of the renamed files and directory path," and

"writing the output of [a virus-checking program] into the mail message in place of the respective encoded portions and sending that mail message" (Col. 12, lines 46-56 – emphasis added). Appellant respectfully asserts that converting attachments "into a format readable by the client," as in Rudd, is quite different from sending messages unchanged, deleting portions of messages, storing portions of messages as files, and writing the output of virus-checking programs into the message, as in Ji. Thus, appellant again respectfully asserts that there would have been no suggestion or motivation to combine the aforementioned references.

More importantly, with respect to the third element of the *prima facie* case of obviousness, appellant respectfully asserts that the combination of the Ji and Rudd references fail to meet all of appellant's claim limitations. For example, with respect to independent Claim 4, the Examiner has relied on Col. 11, line 14-Col. 12, line 67, and specifically Col. 12, lines 47-49 and 56-67 in Ji to make a prior art showing of appellant's claimed "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that ensures that a computer virus in the electronic file is unable to harm a computer of the intended recipient, said converting of the electronic file being in response to a determination that the electronic file represents at least a potential security risk to the computer."

Appellant respectfully asserts that such excerpts only teach "transfer[ring] the mail message with the encoded portions…[with] the viruses deleted…renam[ing] the encode portions of the message containing viruses, stor[ing] the renamed portions as files…and notify[ing] the user of the renamed files and directory path" (emphasis added). Thus, Ji teaches deleting the virus infected portions of a mail message or putting the virus infected portions in a new file and renaming the file. Clearly, since only portions of the file are renamed in Ji, such does not meet appellant's claimed "converting the electronic file," as claimed. Furthermore, Ji only teaches that such infected portions are renamed and stored in files. Simply renaming a file does not meet any sort of converting the format of a file, in the manner specifically claimed by appellant.

In the Office Action mailed 04/18/2006, the Examiner has argued that 'the conversion of the electronic file from a first file format to a second file format includes removing the virus from the attachment which may be in a graphical or word processing format and storing a "treated version" of the file in a format described in Ji as wherein the attachment is "completely cleaned"

which includes "removing the virus from the message" and wherein "the infected attachment…may be replaced with the treated version".' However, merely cleaning the attachment and removing a virus from the message or replacing the infected attachment with the treated version simply fails to even suggest "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension" (emphasis added), as claimed by appellant.

In the Office Action mailed 04/18/2006, the Examiner has further argued that 'the "conversion" that is performed as defined the claim may be done on portions of the file as disclosed in Ji as admitted by the Applicant.' It appears that the Examiner is, in his arguments, relying on appellant's specification to interpret the claimed term "conversion." First, it is noted that appellant claims "converting," not "conversion." Further, in response to the Examiner's proposed claim construction, appellant respectfully asserts that such term should be interpreted under its plain and ordinary meaning, as evidenced by the exemplary definition below, insofar as it is not inconsistent with the specification.

> **convert**
> n.
>
> To change (something) into another form, substance, state, or product; transform: convert water into ice.
> To change (something) from one use, function, or purpose to another; adapt to a new or different purpose: convert a forest into farmland.
>
> *The American Heritage® Dictionary of the English Language, Fourth Edition*
> *Copyright © 2000 by Houghton Mifflin Company.*
> *Published by Houghton Mifflin Company. All rights reserved.*

However, even if the Examiner erroneously relies on the foregoing interpretation of the term "convert," appellant respectfully asserts that the Examiner has still not taken into consideration the full weight and context of such claimed "converting," as noted above. For example, the Examiner has admitted that "Ji discloses that the file retains its original format, the only difference being that the virus is removed." Thus, by virtue of the Examiner's own admission that Ji's file retains its original format, Ji can not even suggest "converting the electronic file

from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension" (emphasis added), as claimed by appellant.

In the Office Action mailed 04/18/2006, the Examiner has additionally argued that "the claims do not specifically require how the electronic file formats are different from each other." The Examiner continued by 'interpret[ing] this difference wherein the first file format with a first file extension is infected with a virus and the second file format is the same file with the virus removed and is considered to be a "safe format" different from the infected format in accordance with the disclosures of the specification.' Again, appellant respectfully disagrees and asserts that the Examiner's argument improperly dismisses appellant's claimed "converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension" (emphasis added), as claimed by appellant. Ji fails to disclose (especially in view of the Examiner's own admission above) that the second file extension is different from the first file extension, in the context claimed by appellant.

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 7

Appellant respectfully asserts that such claim is not met by the prior art for the reasons argued above with respect to Issue #2, Group #1.

Issue # 4:

The Examiner has rejected Claims 22, and 38 under 35 U.S.C. 103(a) as being unpatentable under Ji et al. (U.S. Patent No. 5,889,943) in view of Chen et al. (U.S. Patent No. 5,832,208).

Group #1: Claims 22, and 38

Appellant asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #2, Group #1.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving an electronic file intended for delivery from a sender to an intended recipient, the electronic file having a first file format with a first file extension;

determining whether the electronic file represents at least a potential security risk to a computer system;

if it is determined that the electronic file represents at least the potential security risk, then forwarding to the intended recipient a notification indicating that the electronic file represents at least the potential security risk;

receiving from the intended recipient a request to view the contents of the electronic file;

converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient, said converting of the electronic file being in response to a determination that the electronic file represents at least the potential security risk to the computer system; and

making the converted electronic file available for viewing by the intended recipient.

2. (Original) The method of claim 1, said converting occurring in response to said receiving the request to view the contents of the electronic file.

3. (Previously Presented) The method of claim 1, said converting occurring prior to said receiving the request to view the contents of the electronic file.

4. (Previously Presented) A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving an electronic file intended for delivery from a sender to an intended recipient, the electronic file having a first file format with a first file extension;

converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that ensures that a computer virus in the electronic file is unable to harm a computer of the intended recipient, said converting of the electronic file being in response to a determination that the electronic file represents at least a potential security risk to the computer; and

forwarding a uniform resource locator to the intended recipient of the electronic file, the uniform resource locator identifying at least an address of a web page containing the converted electronic file.

5. (Original) The method of claim 4, the second file format being a HTML file format without scripts.

6. (Previously Presented) A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving a certain electronic file intended for delivery from a sender to an intended recipient, the electronic file having a first file format with a first file extension;

converting the certain electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that prevents a computer virus in the certain electronic file from executing when the converted electronic file is opened by the intended recipient, said converting of the electronic file being in response to a determination that the electronic file represents at least a potential risk to the computer; and

making the converted electronic file available for viewing by the intended recipient.

7. (Original) The method of claim 6, said making the converted electronic file available for viewing comprising:

forwarding a uniform resource locator to the intended recipient of the electronic file, the uniform resource locator identifying at least an address of a web page containing the converted electronic file.

8. (Original) The method of claim 6, said making the converted electronic file available for viewing comprising:

forwarding the converted electronic file to a computer of the intended recipient.

9. (Original) The method of claim 6, said making the converted electronic file available for viewing comprising:

saving the converted electronic file in a memory that is accessible by the intended recipient.

10. (Cancelled)

11. (Previously Presented) The method of claim 6, said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

12. (Previously Presented) The method of claim 6, said determining whether the certain electronic file represents the potential risk comprising:

conducting a heuristic scan of the certain electronic file.

13. (Original) The method of claim 6, the certain electronic file being an attachment to an electronic mail sent over a network.

14. (Original) The method of claim 13, the network including the internet.

15. (Original) The method of claim 6, said receiving occurring at a desktop computer of the intended recipient.

16. (Original) The method of claim 6, said receiving occurring at a server computer.

17. (Original) The method of claim 6, said receiving occurring at a gateway computer.

18. (Original) The method of claim 6, said converting occurring at a desktop computer of the intended recipient.

19. (Original) The method of claim 6, said converting occurring at a server computer.

20. (Original) The method of claim 6, said converting occurring at a gateway computer.

21. (Original) The method of claim 6, the certain electronic file being a first electronic file, further comprising:

receiving a second electronic file intended for delivery from another sender to another intended recipient, the second electronic file having a third file format and containing another computer virus;

converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient; and

making the converted second electronic file available for viewing by the another intended recipient.

22. (Original) The method of claim 6, the computer virus including a macro virus.

23. (Original) The method of claim 6, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

24. (Original) The method of claim 23, the second file format being the HTML file format without scripts.

25. (Original) The method of claim 23, the second file format being the ACSII file format file.

26. (Original) The method of claim 23, the second file format being the TXT file format.

27. (Original) The method of claim 6, the second file format being a file format having text without scripts.

28. (Original) The method of claim 6, the certain electronic file being at least one of a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file.

29. (Original) The method of claim 6, further comprising:

determining if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, the HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

30. (Previously Presented) The method of claim 6, the certain electronic file being an electronic file received by at least one of a FTP transfer protocol or a HTTP transfer protocol.

31. (Previously Presented) A method comprising:

receiving a request to view the contents of an electronic file infected with a computer virus, the electronic file having a first file format with a first file extension; and

in response to the request, converting the electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that prevents the computer virus from executing when the converted electronic file is opened, said converting of the electronic file being in further response to a determination that the electronic file represents at least a potential security risk to a computer.

32. (Original) The method of claim 31, in further response to the request, making the converted electronic file available for viewing by an entity that requested to view the contents of the certain electronic file.

33. (Previously Presented) A computer-readable medium having instructions stored thereon, the instructions when executed by a computer cause the computer to:

convert an electronic file from a first format with a first file extension to a second file format with a second file extension, the electronic file being intended for delivery from a sender to an intended recipient, the second file format with the second file extension being different from the first file format with the first file extension and preventing a computer virus in the electronic file from executing when the converted electronic file is opened by an intended recipient of the electronic file, said converting of the electronic file being in response to a determination that the electronic file represents at least a potential risk to the computer; and

make the converted electronic file available for viewing by the intended recipient.

34. (Original) The computer-readable medium of claim 33, the certain electronic file being an attachment to an electronic mail sent over a network.

35. (Cancelled)

36. (Previously Presented) The computer-readable medium of claim 33 said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

37. (Previously Presented) The computer-readable medium of claim 33, the instructions when executed by the computer further cause the computer to:

determine if the first file format is one of a word processing format type and a graphics format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the first file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

38. (Original) The computer-readable medium of claim 33, the computer virus being a macro virus.

39. (Original) The computer-readable medium of claim 33, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

40. (Previously Presented) An apparatus comprising:

a computer having means for receiving a certain electronic file intended for delivery from a sender to a intended recipient, the certain electronic file having a first file format with a first file extension and containing a computer virus, the computer further including means for converting the certain electronic file from the first file format with the first file extension to a second file format with a second file extension that is different from the first file format with the first file extension and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient, said converting of the electronic file being in response to a determination that a electronic file represents at least a potential security risk to the computer, the computer further including means for making the converted electronic file available for viewing by the intended recipient.

41. (Original) The apparatus of claim 40, said computer being a desktop computer of the intended recipient.

42. (Original) The apparatus of claim 40, said computer being a server computer of a local area network.

43. (Original) The apparatus of claim 40, said computer being a gateway computer.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

Since no decision(s) has been rendered in such proceeding(s), no material is included in this Related Proceedings Appendix.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P091/01.049.01).

Respectfully submitted,

By: /KEVINZILKA/ Date: December 13, 2006

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660